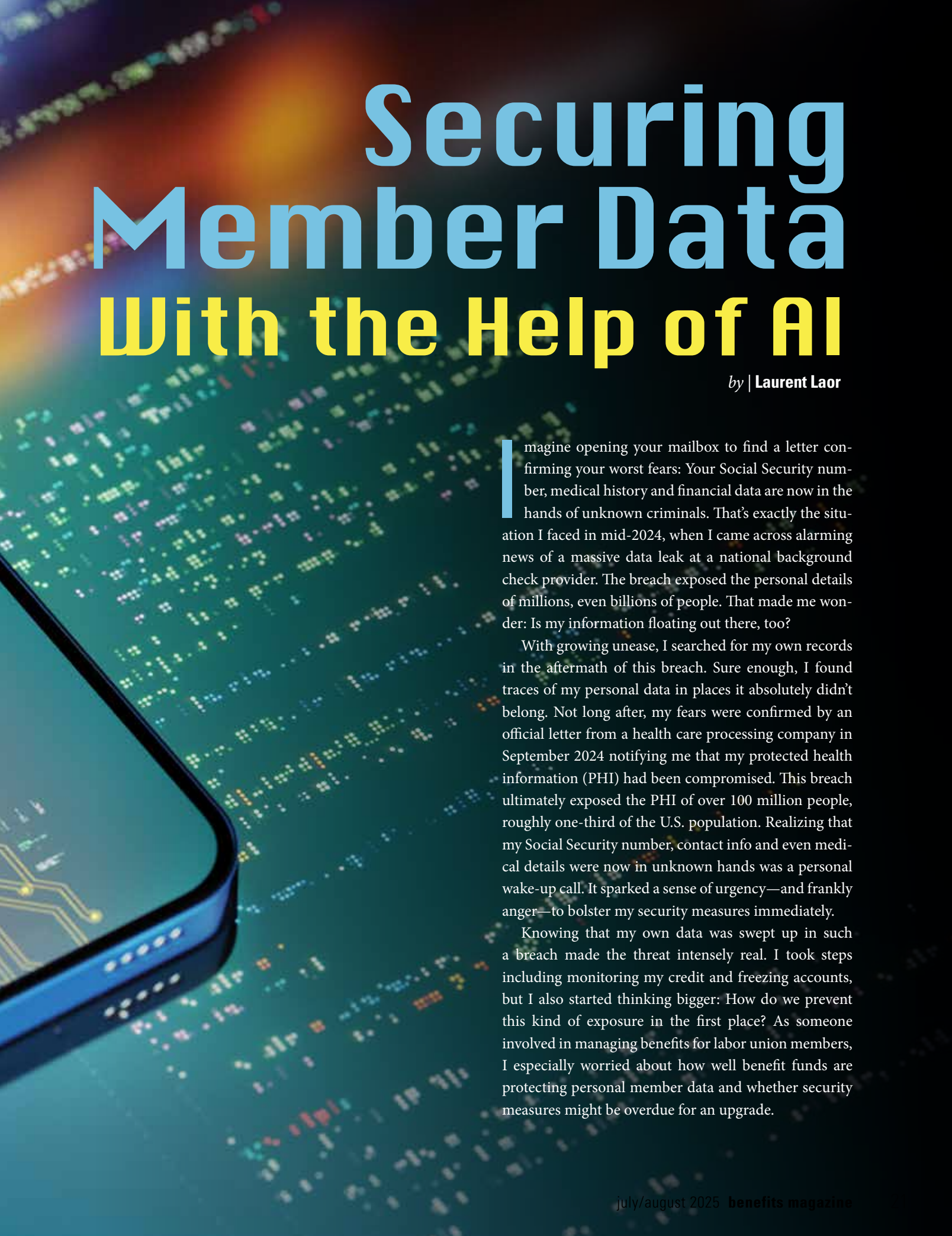
benefits
MAGAZINE

The increase in the number and sophistication of cyberattacks has made it increasingly difficult to protect employee benefit plan member data. Artificial intelligence (AI) holds promise for better data security while improving members' experience.



Securing Member Data With the Help of AI

by | **Laurent Laor**

Imagine opening your mailbox to find a letter confirming your worst fears: Your Social Security number, medical history and financial data are now in the hands of unknown criminals. That's exactly the situation I faced in mid-2024, when I came across alarming news of a massive data leak at a national background check provider. The breach exposed the personal details of millions, even billions of people. That made me wonder: Is my information floating out there, too?

With growing unease, I searched for my own records in the aftermath of this breach. Sure enough, I found traces of my personal data in places it absolutely didn't belong. Not long after, my fears were confirmed by an official letter from a health care processing company in September 2024 notifying me that my protected health information (PHI) had been compromised. This breach ultimately exposed the PHI of over 100 million people, roughly one-third of the U.S. population. Realizing that my Social Security number, contact info and even medical details were now in unknown hands was a personal wake-up call. It sparked a sense of urgency—and frankly anger—to bolster my security measures immediately.

Knowing that my own data was swept up in such a breach made the threat intensely real. I took steps including monitoring my credit and freezing accounts, but I also started thinking bigger: How do we prevent this kind of exposure in the first place? As someone involved in managing benefits for labor union members, I especially worried about how well benefit funds are protecting personal member data and whether security measures might be overdue for an upgrade.

Security vs. Usability: Lessons From a Health Fair

Around that time, a candid conversation at a union health fair drove home another critical point. I spoke with several members about how they access their benefits information online. One older retiree admitted that he avoids the benefits app whenever possible because he dreads the hassle of resetting a forgotten password. Another member joked that logging in to check his health fund status feels like trying to break into Fort Knox, given all the security hoops to jump through. Their frustration was palpable.

This highlighted a key dilemma that benefit plans face: They need strong security to protect sensitive health and pension data, but if the process is too cumbersome, people either won't use it or will find risky work-arounds. At the health fair, I saw usability challenges up close. Plan members want simplicity. They don't want to remember complex passwords or carry security tokens just to get their work and health information. Yet, after my breach scare, I knew that security shouldn't be taken lightly. How can benefit plans strike a balance where plan member data stays safe and members can easily access their benefits?

AI-Driven Authentication: A Potential Game Changer

The answer to this security-versus-usability puzzle may lie in next-generation, AI-powered authentication. Imagine if signing up for a benefits app was as simple as taking a photo of your ID and snapping a selfie and, from that point on, logging in was nearly instant with just your face or fingerprint. It sounds futuristic, but these technologies are available today and could revolutionize how members interact with their benefits. Here's one three-step approach that is being used by several identity management software providers.

1. **ID scan and verification:** Instead of forcing a new user to create passwords and security questions, the user scans their government-issued photo ID (such as a driver's license) using a phone or webcam. Advanced software, backed by AI, instantly checks the ID's authenticity—confirming that the document is valid and not a forgery. The system automatically reads the necessary details (name, date of birth, etc.) from the ID, reducing manual data entry. This step establishes a foundation of trust by tying the account to a verified, real-world identity.
2. **Liveness selfie check:** Next comes a quick selfie, but with an important twist: The user is prompted to take a live selfie (often blinking or turning their head as instructed). The AI system analyzes the selfie and matches it against the photo ID image to ensure that the person is the same individual and is physically present. This liveness detection prevents someone from using a stolen ID or a static photo to impersonate the member. It's even sophisticated enough to thwart deepfakes—an increasingly common fraud tactic. Criminals have started using AI "deepfake" videos and images to spoof identities, with such attacks rising 31-fold from 2022 to 2023.[1] By analyzing subtle cues including skin texture, shadows and motion, the system can tell a genuine live person apart from a fake, catching inconsistencies that a human eye might miss. This step adds a powerful proof: You are who you claim to be.
3. **Secure biometric log-in:** Once the ID and selfie are verified, the member's account is officially confirmed. Now they can dispense with passwords altogether. The user sets up a biometric log-in method for future access, typically using their smartphone's built-in fingerprint or facial recognition. From then on, logging in is as easy as a touch or glance. No more passwords to remember or reset. This isn't uncharted territory; the federal Thrift Savings Plan (TSP) rolled out fingerprint and face log-in for its users in 2024, touting that you can now log in "quickly and securely" with biometrics.

takeaways

- Employee benefit plans have a responsibility to protect plan member data but also need to find ways to make it convenient for members to access benefit services.
- Authentication methods powered by artificial intelligence (AI) may be a big part of the solution.
- One process being used by identity management software providers allows members to scan and authenticate their identification, take a live selfie and create a secure biometric log-in.
- AI verification can spot forged IDs or falsified documents by detecting anomalies that a human might miss and can greatly reduce the risk of account takeovers.
- Plans should make sure that identity verification vendors adhere to Health Insurance Portability and Accountability Act (HIPAA) standards as well as the National Institute of Standards and Technology (NIST) guidelines on digital identity to ensure that they are following best practices.

For multiemployer plan participants, it means that accessing their health or pension info could be as straightforward as unlocking their phone, but with security that meets high standards.

Integrating these steps creates a streamlined yet high-security log-in flow. The first two steps (ID plus selfie) happen just once during enrollment, establishing a trusted identity for the individual. It's a bit like a digital "notary" process—The system has proof of who you are. After that, every log-in is low-effort. The biometric check confirms it's still you, without any typing or codes. From a user's perspective, it's convenient and quick. From a security perspective, it's light years ahead of the old username-and-password approach.

Built to Thwart Modern Fraud and Protect Data

Crucially, this AI-driven authentication is not just convenient, it's designed to defeat modern fraud schemes and protect sensitive data in line with strict regulations. The AI verification can spot forged IDs or doctored documents by detecting anomalies that a human might miss. The selfie liveness check, as mentioned, helps ensure that nobody is duping the system with a picture of someone else or an AI-generated fake. These measures should greatly reduce the risk of account takeovers because an attacker would need to possess an exact match of the victim's physical identity, which is a far taller order than simply stealing a password.

From a fraud-prevention standpoint, this approach closes many of the gaps that hackers and identity thieves have exploited in the past. Weak or reused passwords? No longer an issue. Phishing attacks to trick users out of credentials? A phony email can't steal your face. Social engineering won't easily bypass a live biometric check. And those knowledge-based security questions (like your mother's maiden name or first car) that hackers often glean from public data become obsolete. By leveraging something you have (your government ID) and something you are (your biometric traits) instead of just something you know (a password), vendors adhere to a true multifactor authentication model that is inherently more secure.

Any system that stores plan member data must treat privacy and compliance as nonnegotiables—especially when that data includes medical details. Health plan vendors are legally bound by the Health Insurance Portability and Accountability Act (HIPAA) and similar regulations to safeguard protected health information (PHI); the best go further, aligning their security programs with gold-standard frameworks, such as the National Institute of Standards and Technology (NIST) Digital Identity Guidelines (SP 800-63).

In practice, every piece of personal data—photo IDs, biometric templates, you name it—should be encrypted and managed under strict data-protection rules. The goal is to strengthen security without sacrificing privacy. Take biometric log-ins: They can be designed so the fingerprint or

Setting Up and Using AI Authentication Systems

Employee benefit plan sponsors may want to consider the following when pursuing an authentication system driven by artificial intelligence (AI).

- Look for systems that incorporate government-issued identification and liveness detection to reduce the chances that someone will use a stolen ID or photo to impersonate a member.
- Consider systems that also create a more user-friendly experience for members, such as allowing them to use their smartphone fingerprint or facial recognition to access the system once they've set up their log-in information.
- Ensure that systems have strong encryption protocols and secure storage practices for member data.
- Confirm that the system adheres to health care security regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), which mandate protecting patients' health data.
- Find out whether vendors follow industry standards, such as National Institute of Standards and Technology (NIST) guidelines on digital identity, to ensure that they're following best practices.
- Inform plan members of how the plan will collect, use and retain their personal information.
- Conduct periodic security audits.

learn more

Education

Creating a Culture of Ownership in the Era of AI On-Demand Webcast
Visit *www.ifebp.org/webcasts* for more details.

Online Resource

AI/ChatGPT Toolkit
Visit *www.ifebp.org/toolkits* for more information.

facial scan never leaves the user's device or, if stored, remains in an encrypted form that even system administrators can't decrypt, sharply reducing the risk of exposure.

NIST's *Digital Identity Guidelines* place their highest assurance on a two-step test: Validate a government ID, then match it to a live biometric scan. Solid encryption and secure storage are essential, but transparency matters just as much. The Identity Management Institute advises any group using biometrics to spell out—in plain language—what data is taken, why it's needed, how long it stays and when it disappears. Just as crucial, independent security audits should be scheduled regularly to verify that these promises still hold.

Adopting biometric authentication directly addresses common plan member frustrations—including cumbersome password resets and complicated log-in processes—enhancing both security and ease of use. By embracing advanced biometrics, vendors can deliver the seamless, secure access that members deserve, reinforcing their trust in how benefits administrators protect their most sensitive information.

Real-World Success: IRS and ID.me

The value of AI-driven biometric authentication is being proven in practice. The Internal Revenue Service (IRS) now partners with a digital identity management solution provider, ID.me, to secure taxpayer accounts. Taxpayers accessing IRS systems are asked to verify their identities simply by uploading a government-issued ID and taking a quick selfie, which the system checks using AI-powered liveness detection to ensure authenticity. This approach emerged out of necessity during the COVID-19 pandemic, amid rising identity theft and fraud targeting government benefits.

IRS officials noted that this approach nearly doubled the success rate of identity verification compared with previous methods. By 2024, more than 130 million people in the United States had been enrolled, significantly cutting fraud—Seven states alone credited use of the verification system with preventing more than $270 billion in fraudulent claims.[2] Such results underscore the practical benefits of upgrading security measures to sensitive information such as employee benefits, demonstrating that robust protection and user-friendly access don't have to be mutually exclusive.

A Safer, Simpler Future for Plan Members

Turning my personal data breach scare into action, I've come to appreciate that modernizing authentication is not only about shielding data from bad actors. It's also about making sure the plan members can get in without headache. In the employee benefits world, especially for plan members who may not be tech-savvy, ease of use is a security feature in itself. If the secure way is also the easy way, people are far more likely to adopt it and stop avoiding or undermining the safeguards.

Pairing AI-based identity proofing with biometric sign-in lets benefit funds harden security and simplify access in one move. The portal opens only after a live fingerprint or face scan matches a verified ID, blocking credential thieves while sparing members the password hassle. The result is a quicker log-in, fewer reset tickets and a dramatic drop in the odds that sensitive benefit data ever leaks.

In the wake of the previously mentioned data breach, it became clear that benefits administrators can't be complacent. Once public, your information is out there for everyone to see, and no one understands that better than those of us who have found our data on the wrong side of a breach. We can't undo those incidents, but we can learn from them. For employee benefit plans, that means proactively embracing stronger authentication methods now—before the next big attack—and staying one step ahead of criminals.

bio

Laurent Laor is the chief executive officer and founder of Viveka Health in New York, New York. He previously was the manager of health analytics at Accenture and the director of hospital information systems at Rockefeller University. He earned an M.Sc. degree from Johns Hopkins University and an M.B.A. degree in health finance from Yale University. He can be reached at laurentlaor@vivekahealth.com.

Endnotes

1. "What Is Deepfake Detection in Banking and Its Role in Anti-Money Laundering?" Infopulse blog. May 31, 2024.
2. "Over 70 million Americans keep themselves safe by verifying their identity through ID.me as AI fraud accelerates." ID.me press release. April 8, 2025.
3. "Biometric Authentication Benefits and Risks." Identity Management Institute Center for Identity Governance blog.

pdf/725